PATENT
00CR029/KE

U.S. PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR HIGH ASSURANCE COMPUTING USING VIRTUAL MACHINES ON GENERAL PURPOSE COMPUTING RESOURCES

BY

DAVID A. GREVE

Express Mail Mailing Label EL548587663US

Date of Deposit September 11, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 on the date indicated above and is addressed to the Commissioner of Patents , Box Patent Application, Washington, D.C. 20231.

Edgar A. McGovern

Typed or printed name of person mailing paper or fee

(Signature of person mailing paper or fee)

CROSS REFERENCE TO RELATED APPLICATION

The present invention relates to an application entitled "Method and System For Monitoring Microprocessor Integrity" by David W. Jensen and Steven E. Koenck, filed on even date herewith and assigned to a common assignee. The contents of such application are incorporated herein in their entirety by reference.

FIELD OF THE INVENTION

The present invention generally relates to computing, and more particularly relates to high assurance computing, and even more particularly relates to methods and systems for obtaining high assurance with commercially available general purpose computing resources.

BACKGROUND OF THE INVENTION

In recent years, especially in the area of avionics, multiple dissimilar general purpose microprocessor architectures have been used to attain a high level of assurance of integrity of general purpose microprocessor performance. These multiple processors are used in parallel, and their outputs are compared to reduce the likelihood of an undetected processor failure.

While these multiple dissimilar microprocessor architectures have been used extensively in the past, they do have some drawbacks. First of all, these architectures often use commercially available general purpose processors because of their relatively high performance and low cost. However, these processors, with their ever-increasing size, have increased capacity for bugs or defects. Therefore, with each increase in microprocessor size, which is heralded by the PC community, there is an actual reduction in assurance level. Additionally, when attempting to run the same program on dissimilar processors for avionics equipment, it is necessary to compile and maintain, over the service life of the product (which can often be in excess of thirty years), distinct versions for each of the dissimilar processors. This can be expensive.

Yet another drawback of dissimilar processors is the level of complexity typically involved in achieving communication between the dissimilar processors.

Consequently, there exists a need for economically efficient improved methods and systems for providing enhanced microprocessor integrity without the need for maintaining multiple versions of each of the various applications which run on the multiple processor system.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a system and method for economically enhancing the integrity of microprocessors.

It is a feature of the present invention to utilize a virtual machine, operating on a well-defined subset of the complete instruction set available to the microprocessor.

It is another feature of the present invention to use virtual machines on two dissimilar microprocessors.

It is an advantage of the present invention to limit, through the virtual machine abstraction layer, the set of instructions and/or the condition of their use in a microprocessor, and thereby increase assurance levels for the application and microprocessor combination.

It is another advantage of the present invention to achieve a "lingua franca" or common language, and thereby eliminate the need for multiple compiled versions of each application used on a multiple dissimilar processor architecture and the concomitant expenses associated therewith.

It is yet another advantage of the present invention to reduce processor interface complexity and to provide for fault tolerance in an efficient manner at a level below the application layer.

The present invention is an apparatus and method for enhancing the integrity of general purpose microprocessors which are designed to satisfy the aforementioned needs, provide the previously stated objects, include the above-listed features, and achieve the already articulated advantages. The present invention is carried out in a "multiple compiled application-less" manner in a sense that the need to compile multiple versions of each application used on multiple dissimilar microprocessors has been eliminated. Additionally, the present invention is carried out in a "corner case-less" system in the sense that the defects or bugs which can exist between unusual interactions between instructions or between instructions and asynchronous events (the "corner cases"), can be reduced, via the use of a virtual machine operating with a well-defined and verifiable subset of the complete instruction set for each microprocessor used. When "subset of complete instruction set" is used herein, it is intended to include the conditions of use of such instruction sets as well.

Accordingly, the present invention is an improved computing system and method including a virtual machine operated on a general purpose microprocessor with the intent of increasing the assurance level of the computing system.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may be more fully understood by reading the following description of the preferred embodiments of the invention, in conjunction with the appended drawings wherein:

Figure 1 is a block diagram view of a system of the prior art.

Figure 2 is a block diagram view of a system of the present invention.

Figure 3 is a block diagram view of an alternate embodiment of the present invention which includes single RAM and ROM memories shared by both microprocessors.

DETAILED DESCRIPTION

Now referring to the drawings wherein like numerals refer to like matter throughout, and more specifically referring to Figure 1, there is shown a system of the prior art generally designated 100, including a first prior art general purpose commercially available microprocessor 102, such as an Intel Pentium microprocessor, a dissimilar second prior art general purpose commercially available microprocessor 104, such as a Motorola Power PC microprocessor and a comparator 106, for comparing outputs of first prior art general purpose commercially available microprocessor 102 and second prior art general purpose commercially available microprocessor 104, to determine they are the same and thereby determine that no faults have occurred. Each of the microprocessors 102 and 104 requires a distinct compiled version of each application to be run on the system 100. Each of these compiled versions of the application run on the dissimilar microprocessors is capable of using every instruction set on such microprocessor, including bugs or defects, found in the "corner cases."

Now referring to Figure 2, there is shown a simplified block diagram of a preferred embodiment of the present invention which can be an airborne avionics computing system, generally designated 200, including a general purpose commercially available microprocessor 202, such as, but not limited to, Intel Pentium processors, Motorola Power PC, TI DSPs, etc. The terms "general purpose" are used herein to refer to microprocessors which have a wide range of applicability and are not primarily designed for use in very limited and specific

applications. The terms "commercially available" are used herein to refer to microprocessors which are available for purchase in commercial, wholesale, and retail markets in the U.S. While these processors have widespread acceptance in the industry, these processors also are susceptible to faults which can produce computational errors during normal operation.

Microprocessor 202 is shown disposed on a chip 203, which includes ROM 206 and RAM 208. The term "chip" as used throughout this specification may be a single chip or distributed across two or more devices. The ROM 206 may be used to store the code for the first virtual machine run on microprocessor 202. RAM 208 may be used for various well-known purposes, including scratchpad memory, etc. Of course, this is merely a preferred embodiment of the present invention, and various other approaches could be used as well. The most significant aspect of the present invention is that a first virtual machine is run on microprocessor 202. This first virtual machine then runs the avionics application thereon, on a well-defined, well-tested subset of the entire instruction set available on the microprocessor 202.

To address the diminution in integrity resulting from both known and latent faults, there is included a second high performance general purpose microprocessor 204, which is similar, but not the same make and model as microprocessor 202. Microprocessor 204 is shown disposed on a chip 205, containing ROM 207 and RAM 209, which may or may not be identical to ROM

206 and RAM 208 on chip 203. Microprocessor 204 contains a second virtual machine in ROM 207.

The first virtual machine and the second virtual machine could be identical except that they are compiled to run on the dissimilar microprocessors 202 and 204. In a preferred embodiment, the first and second virtual machines will be, in many ways, very similar to each other. However, due to the dissimilar processors upon which they run, they will operate on a dissimilar subset of instructions. Each virtual machine will operate on a subset of instructions which is well defined and well tested for their respective microprocessor.

Second virtual machine executes, in a parallel fashion, preferably an identical avionics application, which is also run on first virtual machine of microprocessor 202. Said identical avionics application can be stored in ROM 206 for microprocessor 202 and in ROM 207 for microprocessor 204. Alternatively, as shown in an alternate configuration of Figure 3, there is shown a first chip 303 having a microprocessor 202, RAM 208, and a ROM 306, for storing a first virtual machine. Also shown is a second chip 305 having a microprocessor 204, RAM 209, and a ROM 307 for storing a second virtual machine. The avionics application could be a single copy which is stored in ROM 213, depending on trade-offs made by the designer regarding performance and fault tolerance. Identical avionics application could be any type of avionics application, including but not limited to, flight management system applications, flight control computer applications, navigation equipment applications, etc.

The common instruction set of first and second virtual machines thus becomes a "lingua franca" or common language across the dissimilar microprocessors 202 and 204. The outputs of chips 203 and 205 are provided to sync/vote function 210, which may be another microprocessor, a programmable logic device or any other device or combination of devices which can first sync up these outputs and then vote their results. Syncing/voting devices are well known in the prior art and are shown in Figure 1 as comparator 106. When individually compiled applications are run directly on dissimilar processors, as is shown in Figure 1, the comparator 106 is relatively complex. With the use of first and second virtual machines of the present invention, the outputs of microprocessors 202 and 204 are identical. However, these outputs may be skewed slightly over time, because of the dissimilar nature of microprocessors 202 and 204. One of the distinct advantages of the present invention is that some of the complexity (and, therefore, cost) of comparator 106 (Figure 1) can be omitted from the Sync/ Vote function 210, of the present invention. Finally, to attain improved assurance levels, these outputs are voted before they can modify the shared memory 212.

To assure that the outputs of microprocessor 202 and 204 do not diverge over time, a common source of input values for use by microprocessors 202 and 204 is provided through hardware interface 214. This input information is supplied through the sync/vote function 210 so as to provide each microprocessor 202 and 204 with the identical information at the same time.

A preferred method of designing and operating the system of the present invention is described below:

A first microprocessor 202 is provided.

A first FAA certified avionics application is provided.

A first virtual machine is executed on said microprocessor 202 and the first virtual machine executes said first FAA certified avionics application.

A first instruction subset of the first complete set of instructions available to the first microprocessor 202 is defined. This subset omits certain predetermined instructions which are known or likely to produce bugs and defects. The subset also omits certain predetermined instructions which are not essential to running the first virtual machine.

The first virtual machine with its first instruction subset is thoroughly tested and a first verifiable written claim of an improved level of assurance (with respect to use of the first microprocessor without a virtual machine) is made to the FAA for the first virtual machine.

A first certification of the first virtual machine is obtained from the FAA.

In a preferred embodiment, the process is repeated with a second microprocessor 204, second virtual machine, a second instruction subset, a second complete set of instructions, a second verifiable claim and a second certification.

The first and second microprocessors 202 and 204, respectively, are coupled through a synchronizing and voting function 210 before a change is made to shared memory 212.

Throughout this discussion, the terms "certified", "verified" or "determined" or variations of these terms, with respect to the FAA or agency of the U.S. government which regulates air safety shall mean any certification, verification or determination made by such agency irrespective of whether its official designation is the same. Any determination by such agency which follows any inquiry or inspection by said agency, shall be construed as being "certified", "verified" or "determined" by such agency.

While the present invention is believed to be most beneficial for use in aviation and areas regulated by the FAA, it is intended that the present invention could also be used in other areas which are under government regulation, such as, but not limited to nuclear energy and Nuclear Regulator Commission, automotive, rail, and their respective regulatory agencies, as well as OSHA regulations.

Similarly, the present invention is intended to include areas under the control of regulatory agencies of foreign countries and any non-governmental regulatory agency.

It is thought that the method and apparatus of the present invention will be understood from the foregoing description and that it will be apparent that various

changes may be made in the form, construct steps, and arrangement of the parts and steps thereof, without departing from the spirit and scope of the invention or sacrificing all of their material advantages. The form herein described is merely a preferred exemplary embodiment thereof.